Systemic Policy Compliance in a Multi-Jurisdictional Defence Program – Defence Suppliers Perspective

Jean-Paul BUU-SAO, Vijay Takanti, Roel Vester
7 allée Charles Malpel
31300 Toulouse
FRANCE

jean-paul.buu-sao@exostar.com; Vijay.takanti@exostar.com; RHP.Vester@mindef.nl

ABSTRACT

Background

Contemporary Aeronautical & Defense (A&D) programs require customers (defense agencies) and their suppliers to collaborate in environments that involve partners globally spread over the globe. In such a broad multi-jurisdictional environment, there is an increasingly critical need to ensure that all applicable information protection policies are enforced throughout the lifecycle of the programs, from concept to design, manufacturing, support and program end-of-life. These information protection policies come from multiple sources, such as: national policy authorities, that define policies aimed to protect national security interests, export control policy authorities, that define policies aimed at controlling the export of sensitive goods and information to foreign countries, and corporate policy authorities, that define policies aimed at protecting corporation's intellectual properties.

The Transglobal Secure Collaboration program (TSCP, http://www.tscp.org) is a consortium that is formed by major industrial players that serve the aeronautical and defense sector, together with government organizations; their customers. This consortium aims at developing governance, common operating rules and technical specifications that can be used to implement a scalable and interoperable collaboration capability that is compliant with the appropriate policies that govern such systems.

In this context, the TSCP has to address a number of collaboration scenarios where information is protected, while allowing for efficient sharing. This paper focuses on some of the issues related to the automation of information protection enforcement, including: the modelling of information protection policies, and the expressiveness required from authorization languages. Although this paper presents a solution framework that addresses the acquisition scenario, the solution framework presented in this paper is useful in other defense industry scenarios as well.

What we did

We established a framework related for the management of information protection in the context of information sharing that needs to comply with a number of policies. These policies are specified by the organizations involved in the collaboration as well the regulatory authorities that govern sharing of sensitive information across national boundaries. This framework includes a modeling of the use-cases related to information protection policies, encompassing administrative and execution considerations. The use-cases were put together with the help of enterprise architects from the major A&D organizations and National Defense agencies, and at this stage being validated by Subject Matter Experts from A&D organizations. The framework includes a data model derived from the use-cases, and which supported the articulation of the policies, such as United States export control license agreements, and organization intellectual protection policies. Lastly, the framework includes an XML-based interchange representation of the information protection policies, allowing the exchange of policy terms across autonomous enterprise boundaries.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2010	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Systemic Policy Compliance in a Multi-Jurisdictional Defence Program Defence Suppliers Perspective	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **7 allée Charles Malpel 31300 Toulouse FRANCE**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADA564697. Information Assurance and Cyber Defence (Assurance de l'information et cyberdefense). RTO-MP-IST-091

14. ABSTRACT

Contemporary Aeronautical & Defense (A&D) programs require customers (defense agencies) and their suppliers to collaborate in environments that involve partners globally spread over the globe. In such a broad multi-jurisdictional environment, there is an increasingly critical need to ensure that all applicable information protection policies are enforced throughout the lifecycle of the programs, from concept to design, manufacturing, support and program end-of-life. These information protection policies come from multiple sources, such as: national policy authorities, that define policies aimed to protect national security interests, export control policy authorities, that define policies aimed at controlling the export of sensitive goods and information to foreign countries, and corporate policy authorities, that define policies aimed at protecting corporations intellectual properties. The Transglobal Secure Collaboration program (TSCP, http://www.tscp.org) is a consortium that is formed by major industrial players that serve the aeronautical and defense sector, together with government organizations; their customers. This consortium aims at developing governance, common operating rules and technical specifications that can be used to implement a scalable and interoperable collaboration capability that is compliant with the appropriate policies that govern such systems. In this context, the TSCP has to address a number of collaboration scenarios where information is protected, while allowing for efficient sharing. This paper focuses on some of the issues related to the automation of information protection enforcement, including: the modelling of information protection policies, and the expressiveness required from authorization languages. Although this paper presents a solution framework that addresses the acquisition scenario, the solution framework presented in this paper is useful in other defense industry scenarios as well.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**20**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Based on this framework, we implemented technical solutions that could automate the enforcement of the information protection policies within common document sharing applications. More specifically, after considering various forms of authorization paradigms and supporting languages, we selected an Attribute Based Access Control (ABAC) paradigm, with support of the Extensible Access Control Markup Language (XACML). We established how the complex policies derived using our framework, could be translated to XACML policy sets, and evaluated how all required attributes could be delivered for evaluation by the XACML engine in order to provide the appropriate authorization decision. Finally, we looked at the issues of integration of an XACML engine with the collaborative application, with particular interest at issues such as: integrity of policy binding, performance and caching.

What we found

There are many XACML implementations currently available, including out-of-the-box Policy Enforcement Points integrated well in commercial applications such as in prominent web-based document management systems. However these implementations invariably provide a Policy Administration Point that not surprisingly target XACML as a native policy expression language. Our investigations of real world information protection policies have shown that there are requirements that cannot directly be met by a formalism solely driven by access-control rules-set evaluation, such as the one offered by XACML. Some additional challenges, that we needed to consider, included: the capability to distribute the evaluation of the security policy (various evaluations contributing to yield the final result), the verification of its correctness (i.e. prove that the expression meets the intent), and the issue of conflict-resolutions at design-time versus at run-time. This is just the beginning of a journey, but at least we know that the expression of the security policy needs to use formalisms enabling analysis and theorem-proving, such as logic-based policy specification language (e.g. SecPal, Cassandra, DKAL, Ponder etc), from which implementation languages, such as XACML, could be generated.

What this means to the audience

Within each organization authorization management is a 'hot' topic. For governments, just as commercial companies, there are stringent rules for giving access to information. The TSCP development, although initially focused on Intellectual Asset Protection and Export Compliance is developing a capability, based on open standards, that enables anyone to develop Attribute Based Access Control mechanisms, for giving this access. The fact that many big companies in the Aerospace and Defense industry are working with technology leaders such as Microsoft shows that TSCP work is an important development that will be available in standard COTS products in a few years. The TSCP community is now also actively considering approaching the standard organizations such as ISO.

A few NATO member states are currently investigating what TSCP will mean too them, because many Defense Departments have business with companies that are now moving towards TSCP compliance. TSCP member county representatives are also starting to explore how TSCP can be re-used outside of the aerospace and defense industry because TSCP framework is an open specification, which consists of best practices, which can be re-used. Because of this we assume there will be a broader adoption then just the Aerospace and Defense industry, and we expect to see broader adoption of our framework.

1. BACKGROUND OF THE STUDY

1.1 Security Challenges

TSCP is a federation of major Aerospace and Defense organisations around the globe, whose primary objective is to develop an Interoperable Cross-Enterprise Architecture aimed that can support a number of large scale collaboration programs that have to comply with different regulatory policies, whilst mitigating risks associated with information sharing. This complexity of broad collaboration spanning across multi-national regulation environments is further increased by the following considerations:

- Challenges of increasing risk: a characteristic of the supply chain in the Aerospace and Defense industry is the number of trading partners (tiers) involved (depth) and the large regional repartition of these tiers (breadth). With respect to risk expansion, what guarantees that trustor (e.g. information owner) needs to have in place to share information with trustees with whom he might not have a direct relationship, and who are furthermore located in potentially different jurisdictions? The risk, that the trustor needs to take, increases with the sensitivity of the information exchanged, and therefore a lack of trust jeopardizes the operation of the supply-chain.
- Challenges on value-based trust: some A&D industry participants, who are culturally from the civilian sector, are exposed to issues regarding value-based trust, as they see their own information acquire the dual use status (dual use refers to products and technologies which are normally used for civilian purposes but which may have military applications): handling of such dual use information requires adapting the culture, training, processes and toolset, with associated cost impact. It is not surprising that the expansion of the collaboration beyond organisation and regional boundaries raises even further issues to the applicability of value-based trust.
- Challenges on expectation-based trust: expectation-based trust is commonly used in the aerospace and defense industry in context of the sharing of information, whereby the owner of the information has the expectation that the information is handled by all appropriate parties in a way that corresponds to the information owner's protection policies. Issues arise when the collaboration spans across organisations and regions: how can the information owner indicate the intent of use in unambiguous way. If data-tagging techniques are chosen, how to ensure that the data-tag conveys to all parties, a similar intent? The risk of misinterpretation, even in a non-malicious way, of the intent is increasingly larger when crossing organisational and regional boundaries.

The additional exposure to risks, due to the expansion of collaboration across organisations and regional boundaries, is the common theme that we have covered so far.

1.2 Trust Mechanisms

TSCP has been formed with the objective to help address these challenges, by taking the following approach:

- There is a need to impose institution-based trust across the industry;
- There is a need, within each organisation, to translate the institutionalized trust onto system trust, whereby the processes and mechanisms of the organisation contribute to implement the institutionalized trust.

1. Institution-based trust: A hierarchy of Policy Authorities

The formal, legitimized structures for guaranteeing trust are the many Policy Authorities that each individual organisation, participant to the Aerospace and Defense collaboration, need to recognize. Policy Authorities are organizations that own policies, i.e. which are in the position to define, promote and force the enforcement of policies. Policy Authorities impose themselves at different levels, whether pan-national, national, regional or corporate.

Amongst all the relevant Policy Authorities, the additional difficulty is to identify, which specific policies are applicable in the context of the collaboration, given the various jurisdictions which governs the various collaboration partners. The result of this determination will produce some form of aggregation of policies across the relevant Policy Authorities. All this needed to be done before any information exchange can take place, which is to figure out how to apply the policy, both procedurally (via processes, run by human beings) and systemically (run by systems infrastructure).

This problem is sufficiently complex to (already) that it needs the support of a multi-disciplinary team work to identify and develop the various aspects of the solution including: legal, process, technology, product, business and organisational knowledge is needed in order to produce the aggregate of all the policies for a given collaboration context. Once the applicable policies are identified, the next challenge is how to enforce the policies across the number of disparate partners and how to verify compliance?

Given the complexity illustrated above, and in order to ensure trust amongst all the collaboration participants, the option to setup a trusted authority solely aimed to establishing trust has been put forward. The structure, rules of engagement, mission, domains of competence, and operation of this institution are beyond the scope of this discussion.

It is sufficient to mention that such an institution-based trust (or systems trust) cannot function without an appropriate audit regime. The audit regime defines the methodology to demonstrate compliance in a scalable fashion while ensuring that all participants comply with the appropriate policies, , by requiring all participants to be audited by accredited auditors.

Another role of this trusted authority is to ensure the establishment of trust in a scalable manner across all the collaboration participants. This is important in aerospace where a system integrator is complemented by a large number of suppliers, ranging from a select set of first tier suppliers to many third tier suppliers, potentially not even related to the aerospace domain. This scalability can be achieved with multilateral trust, whereby the institution is a trusted tier with whom each participant needs to establish trust bilaterally: establishment of trust becomes scalable as each individual participant needs to perform the heavy-duty qualification only once, with the trusted tier. Then trust is established transitively or indirectly between all participants in the virtual enterprise. This requires the Trusted Authority to become a Policy Authority by itself, with authority to dictate information security policies that all participants of the industry, need to comply with.

2. System-based trust

Trusting systems (run by software) for the enforcement of designated policies is a problem that has been tackled with, ever since the first Operating Systems and still is alive nowadays. The challenges behind this objective are addressed in an incremental way, following the technology evolution. Capable of firstly enforcing very simple policies, systems have evolved with the capability to cope with incrementally more complex policies, and yet, we currently observe that not all policies can be fully enforced by systems solely: a large part of procedural means is still currently required. Nevertheless, one can observe that the evolution of the capability to enforce incrementally more complex policies follows the evolution of the various access control mechanisms, which are largely covered by the literature. This evolution is summarized below:

- Discretionary Access Control (DAC) [1] based-systems could enforce simple policies that can be modelled as matrices of permissions for designated subjects;
- Role Based Access Control (RBAC) [2] systems still enforce policies that can be modelled as matrices of permissions, with the difference from DAC that the matrices does not contains subjects directly, but an abstraction (role) that can be used to group subjects bearing the same characteristic together; in some cases, the concept of inheritance helps simplifying the role of management by establishing hierarchies of roles, which present the caveat to not always accurately model the reality of business roles;
- Attribute Based Access Control (ABAC) [3] systems represent a quantum leap forward by introducing the concepts of rule-set, runtime selection, instantiation and evaluation of the rule-set; this allows to better enforce real-world policies, as long as these can be formalized as rule-set, which is not always possible. In addition to a simple rules-engine, some systems add Artificial

Intelligence mechanisms, such as inference mechanisms and/or the capability to handle fuzzy logic (in addition to predicate logic).

– Organisation Based Access Control (OrBAC) [4] systems start new grounds in leveraging outcome of social and organisational sciences (and not solely computer sciences as for the systems seen above) by introducing constructs, such as context or temporal constraints, that are better suited to enforcing real-world policies.

TSCP has chosen to address the institution-based and system-based trust by specifying a framework for policy and trust management. On the one hand, this framework, which proposes a model for capturing policy artefacts, is a key in the establishment of institution-based trust. On the other hand, this framework promotes and supports automation of policy enforcement, and should be a key contributor to providing system-based trust.

The next two chapters present the framework, then a prototype demonstrating the framework.

2. FRAMEWORK FOR POLICY AND TRUST MANAGEMENT

2.1 Terminology

Policy Authority: an organizational structures that own policies, i.e. which are in the position to define, promote and force the enforcement of policies. Policy Authorities impose themselves at different levels, whether pan-national, national, regional or corporate.

Information protection policy: the aspects of the policies generated by the policy authorities that are concerned with the protection of information.

Mandatory Policy: Enforces access control rules based directly on an individual's clearance, authorization for the information and the confidentiality level of the information being sought. Other indirect factors are physical and environmental. This policy must also accurately reflect the laws, general policies and other relevant guidance from which the rules are derived.

Discretionary Policy: Enforces a consistent set of rules for controlling and limiting access based on identified individuals who have been determined to have a need-to-know for the information.

Procedural policy enforcement: enforcement of policies by the mean of procedures performed by human being, usually as the result of training and awareness of these policies and ability to interpret when to apply the policies.

Systemic policy enforcement: enforcement of policies by the mean of systems, understood as a combination of software and hardware.

Identity Federation: The agreements, standards, and technologies that make identity and entitlements portable across autonomous domains.

2.2 Business Process

The prototype demonstrates a process where policy-authorities express their requirements in a form that is consistent across policy-authorities, and that allows for automated processing by organizations having to comply with these policies.

The figure below depicts a typical Aerospace & Defense (A&D) setting, where, in context of a specific Business Engagement (a Program), an organization playing the role of “Delegated Administrative

Authority" aggregates together all the applicable policy requirements (we use the term:the Protection Profile noted PP, formed by an aggregation of at least two Business Authorizations, noted BA1 and BA2), for all organizations which are part of the program (Organization 1 to 3) to implement.

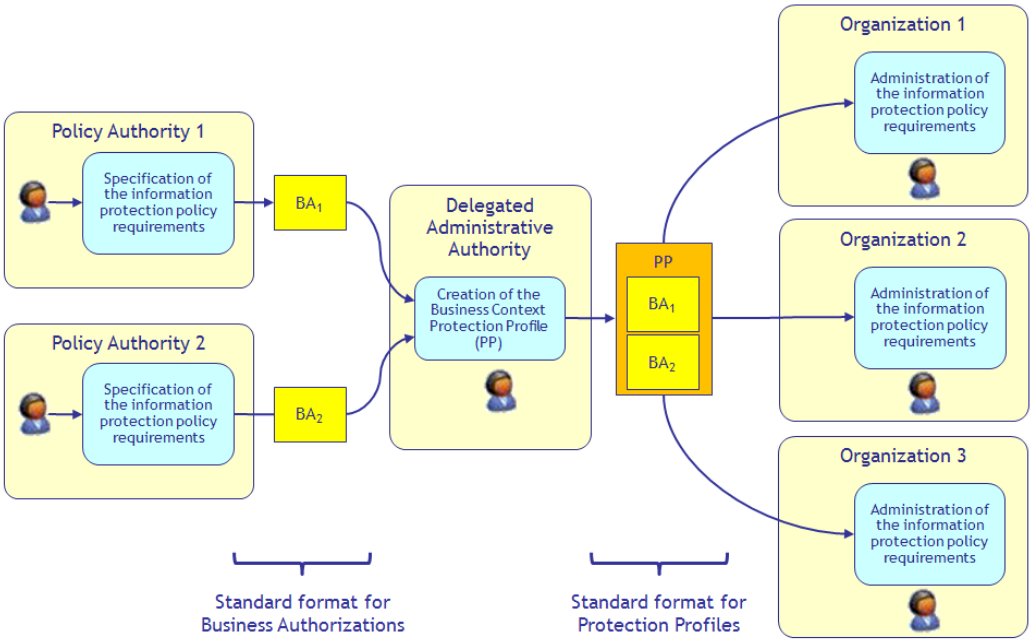

Figure 1: Business Authorization Flow across organizations

The three business key processes implied by this model are:

- Specification of the information protection policy requirements: policy authority administrators formulate their policy requirements in the form of a Business Authorization, which is standard across policy authorities;
- Creation of the Business Context Protection Profile: the organization playing the role of delegated administrative authority puts together the comprehensive set of Business Authorizations applicable to the program, in the form of a Business Context Protection Profile, which is standard across program participants;
- Administration of the information protection policy requirements: organizations that are part of the program need to implement the Business Context Protection Profile before starting to collaborate. This last process is detailed below.

The administration of the information protection policy requirements, within each organization, is managed by: the Business Authorization Management System (BAMS). This system serves as an enterprise repository of Business Authorizations, and is accessed by other systems within the enterprise for systemic enforcement of the Business Authorizations.

The figure below illustrates a typical scenario of policy enforcement:

1) A document owner uses a labeling tool in order to apply a Business Authorization Label (BAL) into a document. The BAL is the link to all the Business Authorizations that need to apply to the document, and is visible to human users (for procedural enforcement) and processable by systems (for systemic enforcement).

2) Once the document is cleared for release, a user uploads the document (with its associated BAL) to a Document Management System. At this point, a first systemic enforcement is performed, as the Document Management System has a Policy Enforcement Point that asks authorization to a Policy Decision Point, passing over the information contained in the BAL. The Policy Decision Point itself evaluates the access rules associated with the BAL. It is assumed that at administration time, the access rules that the Policy Decision Point can evaluate, have been generated from the access rules contained in the Business Authorizations.

3) A user accesses the Document Management System in order to download the document (with its associated BAL). At this point, a second systemic enforcement is performed, using the same mechanism as described above.

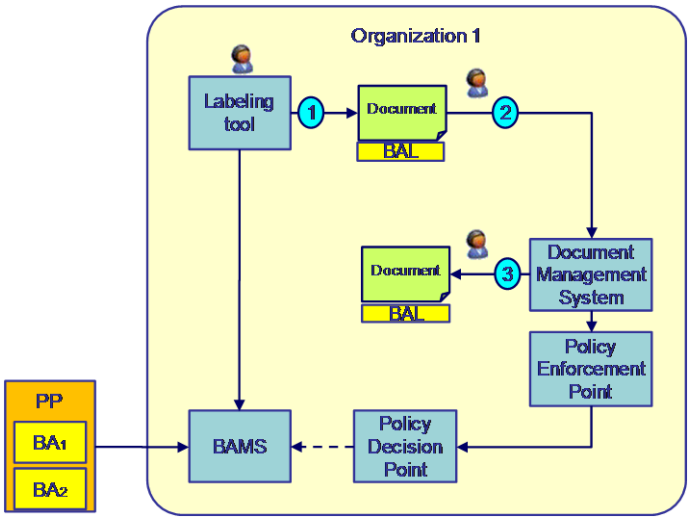

Figure 2: Systemic policy enforcement within one organization

The three-step scenario above, which occurred within one same organization, can also take place across organizations. This is illustrated in the fig below.

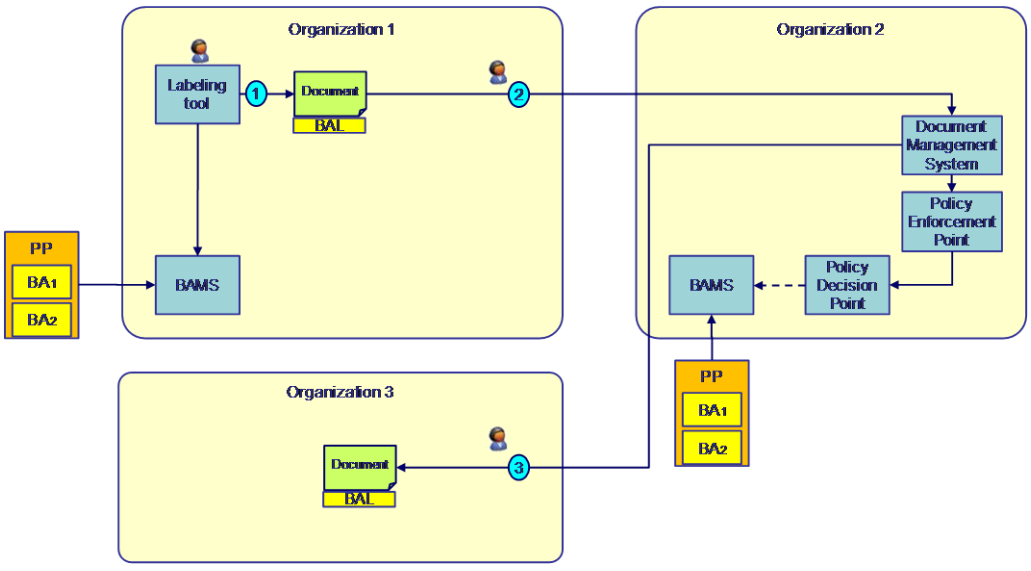

Figure 3: Systemic policy enforcement across organizations

2.3 Business Authorization

The concept of Business Authorization (BA) identified above, captures the primary provisions of information protection policies that need to be enforced. We have taken a pragmatic approach to model Business Authorizations, by abstracting two real world policies: the Technical Assistance Agreement (TAA), part of the export control policy regime under US International Traffic in Arms Regulation (ITAR), and a representative organization specific Proprietary Information Exchange Agreement (PIEA).

A Business Authorization typically has the following attributes:

Administrative attributes

- Applicant and signatories: the parties who executed the Business Authorization and hence have agreed to abide by the rules stated in the authorization
- Cover letter: reference of the Business Authorization at the Policy Authority
- Validity dates

Attributes about the requestor

- Authorized business assignment: a 3-tuple of {Organization Breakdown Structure (OBS), Product Breakdown Structure (PBS), Work Breakdown Structure (WBS)}
- Nationality[1]
- Requestor physical location (country)

Attributes about the resource

- Included (authorized), or excluded (un-authorized) associated item categories, related to a specified category-list, such as ITAR's US Munitions List [5]; in an export control regime, this designates the category of controlled items which the resource (information object) relates to
- Included (authorized), or excluded (un-authorized) associated impact levels, expressed on a specified scale of impact levels, such as FIPS-199 scale of potential impacts **Error! Reference source not found.**

Attributes about the environment

- Level of machine health
- Alert state, such as US Homeland Security Advisory System's color-code, or UK Threat Levels
- Others

Each Business Authorization specifies a set of functions that need to be evaluated in order to render a possible empty, result set, composed of a list of authorized actions.

2.4 Protection Profile

We define "protection profile" as the aggregation of all the information protection policies that are applicable to a given context (e.g. Aerospace & Defense program). The protection profile contains administrative attributes about the profile itself (such as the name and contact of the administrative authority managing this profile), and the list of all applicable protection policies. Each protection policy is

[1] Current EU regulations prevent organizations from asserting privacy related attributes such as requestor's nationality, in which case utilization of derived attributes is required. This aspect is out of scope of this paper.

fully described in terms of administrative attributes (e.g. validity dates), access rules and associated information marking and labelling scheme.

The prototype defines specifications in the form of a data model, as well as an XML-based interchange format for protection profiles, that allow vendors to provide implementations of supporting tools, and allow organization to exchange protection profiles in an interoperable way.

Additionally the prototype includes a prototype-grade implementation for this specification, allowing authoring a protection profile, exchange protection profiles, and search through a protection profile.

2.5 Information Marking and Labelling

We define "information marking" as the process of adding visual indicators to an information object in order to provide to human persons an indicator of the information sensitivity and hence helps in the identification of the applicable protection policies that are applicable, enabling procedural enforcement of these policies.

We define "information labelling" as the process of associating policies to an Information Asset, both for human consumption (procedural policy enforcement), and for system consumption (systemic policy enforcement).

Organizations, most particularly defense ones, currently make a heavy use of information marking by the means of conventional visual marking (e.g. First Line of Text on an Email, Header/Footer keywords on a document), with the assumption that end-users are trained on how to handle the marked information.

Information marking falls short when it comes to providing some level of automation to the policy enforcement, as visual marking is not well suited for systemic interpretation.
Here is where information labelling comes to play: the prototype introduces the concept of a "labelling scheme", which includes the following components:

- Labelling guidelines: instructions that a human person must follow in order to determine which policies need to be attached to an Information object, in a given business context.
- Visual marking: specifies the appearance of visual indicators of the protection policy, for procedural enforcement. The visual marking is in general dependent upon the nature of the information object, and hence need to address all types of information objects under consideration (e.g. how should visual marking appear to the user on an Email, an Office document, a CAD document etc)
- Systemic marking: specifies the metadata that are keys to identifying the protection policy, for systemic enforcement. The systemic marking is in general dependent upon the nature of the information object, and hence need to address all types of information objects under consideration (e.g. how should systemic marking appear to the user on an Email, an Office document, a CAD document etc)

3. PROTOTYPE DEMONSTRATING THE FRAMEWORK

3.1 Functional Architecture

The functional architecture of the prototype is depicted below:

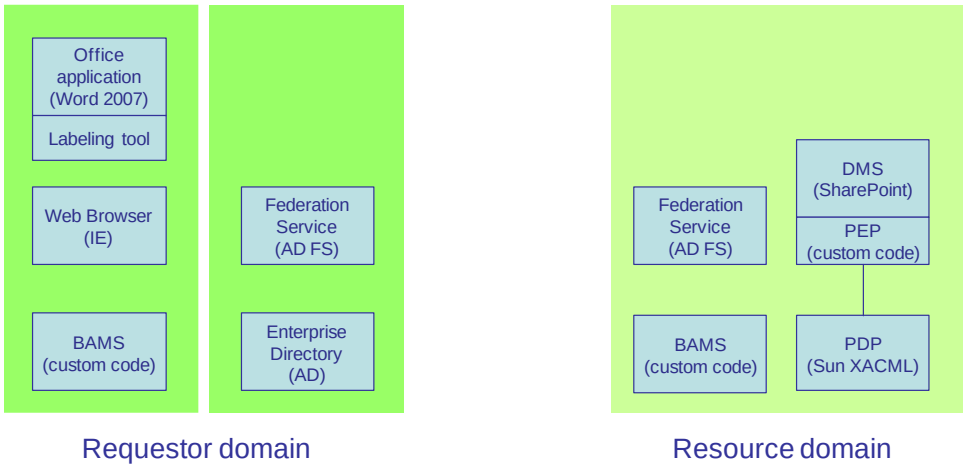

Figure 5: Prototype functional architecture

The requestor domain hosts the functional components needed to create and consume documents:

- An office application is used to create and read documents. The office application includes, as a plug-in, a labelling tool, which function is to assist the user on the determination of the Business Authorization Labels (BAL) that need to be associated to the document, and to apply the BAL to the document in user-readable and machine-readable, forms;
- A Business Authorization Management System (BAMS) is used as a repository for Business Authorizations. The BAMS is accessed by the labelling tool, at the time where the user needs to locate the details of the Business Authorization in order to determine which ones apply to the document;
- A web browser is used in order to communicate with the Document Management System, for uploading and downloading documents;
- A federation service is used in order to create trusted attributes about the user, and convey these attributes to the resource domain, using a standard identity-federation protocol;
- An enterprise directory is used to repose user accounts and business related information, such as user project assignments. Users authenticate by the enterprise directory.

The resource domain hosts the functional components needed for a shared document repository:

- A document management system is used as a shared repository for document; this web-application provides storage for documents, as well as navigation and search functionalities;
- A Policy Enforcement Point (PEP) is used to enforce policies within the document management system; his function is to intercept certain user operations, such as document upload or download, in order to make sure that these operations are authorized in accordance to the applicable policies. The PEP does not take the authorization decision itself, but queries the authorization decision by the Policy Decision Point, passing along the attributes about the user, the resource, and the intended action, needed for the determination of the authorization decision;
- A Policy Decision Point (PDP) is used to generate authorization decisions, based on policy sets contained in a policy store. The prototype uses a XACML[5] rules engine as PDP; hence the policy sets are XACML policies;

- A Business Authorization Management System (BAMS) is used as a repository for Business Authorizations. The BAMS is used out-of-band in order to code-generate the XACML policy sets from the Business Authorizations;
- A federation service is used in order to consume trusted attributes about the user, and convey these attributes to the document management system, using a standard identity-federation protocol.

3.2 Business Scenario

We have demonstrated the prototype by using a business scenario that is representative of a real-world collaboration within the aerospace & defense industry.

Curtiss Corporation, registered and based in the US, has been awarded a United States Air Force (USAF) contract for the delivery of a new fighter jet. Curtiss has chosen to establish partnerships with two organizations in order to deliver a Navigation System: Packard LLC (a UK company specialized in military-grade navigation systems) and Spad (a French company specialized in simulation).

The three organizations collaborate in order to deliver the Navigation System end-product, by executing a number of work items (High-Level-Design, Detailed Design, Simulation and Integration). The figure below shows the relationship between the elements of the Engineering Bills Of Material (that is related to the Product Breakdown Structure, PBS), the Work Breakdown Structure (WBS), and the Organization Breakdown Structure (OBS).

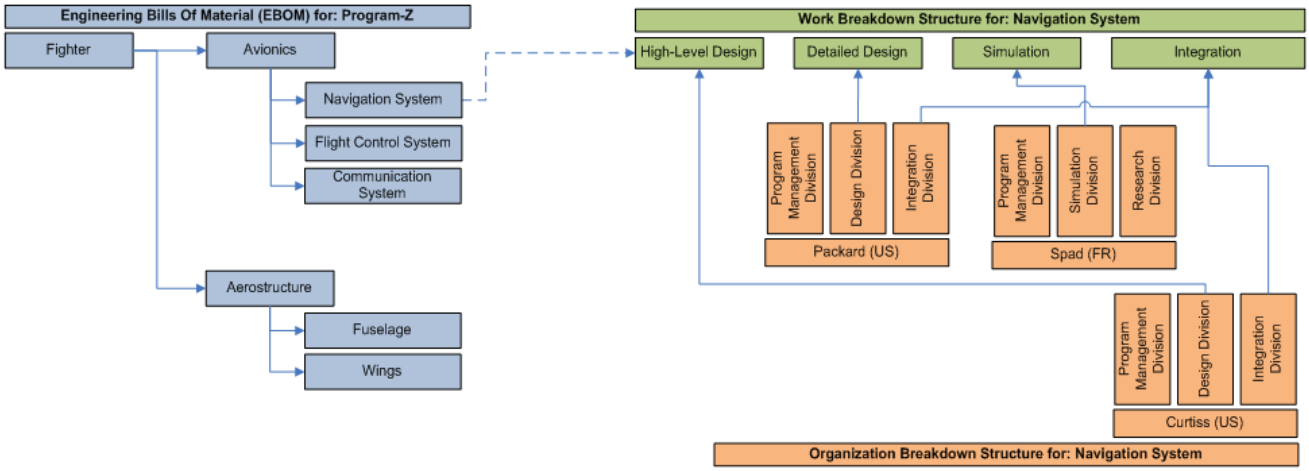

Figure 5: Business scenario context

3.3 Policy Context

The collaboration around the delivery of the Navigation System involves the exchange of product items and of information about product items. All this exchange needs to be secured in accordance to the relevant protection policies. The prototype is only concerned about logical security, hence the protection of information about product items.

Two types of protection policies were modelled:

1. Export Control protection policy, modelled after a typical Technical Assistance Agreement (TAA) from the US ITAR regime. TAA protect the exchange of information about US export controlled items;

2. Intellectual Property protection policy, modelled after representative Proprietary Information Exchange Agreements (PIEA). PIEA protect each other's Intellectual Property exchanged in context of the collaboration.

Any of these two types of protection policies can include two policy components:

- Mandatory policy: what is the risk impact associated to the information? How severe is the impact of the information being compromised? The risk impact needs to be mitigated with the appropriate security controls, which can mandate a minimum level of encryption to level of hardening of the operating systems and applications. The risk impact is expressed as set of values taken from a risk impact scale. The prototype uses the FIPS-199 scale, which defines four values, from level-1 (minimum impact) to level-4 (maximum impact).
- Discretionary policy: who needs to know about the information? The discretionary policy is set at the discretion of the information owner. Discretionary policies are typically expressed as an authorization expression, which articulates attributes associated to the requestor of the information.

The table below shows the protection policies that have been put in place for the prototype:

- Bilateral PIEA1 between Curtiss and Packard
  - Purpose = protects Curtiss IP exchanged with Packard
  - Discretionary policy: allow distribution of IP amongst organization stakeholders
  - Mandatory policy: risk impact = {FIPS-199, Level 1}
    - Curtiss employees assigned to Program-Z HLD or DD can release and read
    - Packard employees assigned to Program-Z DD can read
- Bilateral PIEA2 between Curtiss and Spad
  - Purpose = protects Curtiss IP exchanged with Spad
  - Discretionary policy: allow distribution of IP amongst organization stakeholders
  - Mandatory policy: risk impact = {FIPS-199, Level 1}
    - Curtiss employees assigned to Program-Z DD can release and read
    - Spad employees assigned to Program-Z SIM can read
- Multilateral TAA1 between Curtiss and {Packard, Spad}
  - Purpose = allows Curtiss to export designated controlled information to Packard and Spad
  - Form of agreement: one TAA, signed by all organization stakeholders, for the duration of the program
  - Discretionary policy: allow distribution of US controlled items to designated organization/individuals
  - Mandatory policy: risk impact = {FIPS-199, Level 2}
    - Curtiss and Packard employees physically located in US or GB can release and read
    - Spad employees physically located in FR or GB can read

3.4 Access Control Rules

The access rules, which are declaratively contained in the protection profile, can be translated in an executable form in various authorization languages. For this prototype we have chosen XACML (Extensible Access Control Markup Language)[5] for its availability as an open-source implementation and for its support by the OASIS standards organization. The translation of Business Authorization access rules to XACML policy-sets were firstly performed by-hand. Based on this experience we have gathered sufficient confidence that this translation could be automated by forthcoming commercial products implementing the framework.

For brevity we provide here the translation of the access control rules contained in the first PIEA 1 to a XACML policy.

```
<Policy PolicyId="uri://tscp/ba/PIEA#1.1" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
   <Description>PIEA #1.1: Bilateral PIEA established by Curtiss and allowing access of Curtiss PI to Packard</Description>
   <Target>
   <Resources>
      <Resource>
         <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">uri://tscp/ba/PIEA#1.1</AttributeValue>
            <ResourceAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:policy-id"></ResourceAttributeDesignator>
         </ResourceMatch>
      </Resource>
   </Resources>
   </Target>

   <Rule RuleId='PIEA#1.1:grant:curtiss:DD:update+read' Effect='Permit' xmlns='urn:oasis:names:tc:xacml:2.0:policy:schema:os'>
      <Description>Curtiss employees assigned to Program-Z/HLD+DD can release and read</Description>
      <Target>
         <Actions>
            <Action>
               <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">release</AttributeValue>
                  <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                        DataType="http://www.w3.org/2001/XMLSchema#string"/>
               </ActionMatch>
            </Action>
            <Action>
               <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
                  <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                        DataType="http://www.w3.org/2001/XMLSchema#string"/>
               </ActionMatch>
            </Action>
         </Actions>
      </Target>
      <Condition>
         <Apply FunctionId='urn:oasis:names:tc:xacml:1.0:function:and'>
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member-of">
               <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
                  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">curtiss</AttributeValue>
               </Apply>
               <SubjectAttributeDesignator AttributeId="urn:tscp:subject:organization-affiliation"
                        DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Apply>
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member-of">
               <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
                  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">program-z</AttributeValue>
               </Apply>
               <SubjectAttributeDesignator AttributeId="urn:tscp:subject:assigned-program"
                        DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Apply>
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member-of">
               <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
                  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">DD</AttributeValue>
```

```
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">HLD</AttributeValue>
              </Apply>
              <SubjectAttributeDesignator AttributeId="urn:tscp:subject:assigned-work-effort"
                    DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Apply>
          </Apply>
        </Condition>
      </Rule>

      <Rule RuleId='PIEA#1.1:grant:packard+spad:DD:read' Effect='Permit' xmlns='urn:oasis:names:tc:xacml:2.0:policy:schema:os'>
        <Description>Packard employees assigned to Program-Z/DD can read</Description>
        <Target>
          <Actions>
            <Action>
              <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
                <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                    DataType="http://www.w3.org/2001/XMLSchema#string"/>
              </ActionMatch>
            </Action>
          </Actions>
        </Target>
        <Condition>
          <Apply FunctionId='urn:oasis:names:tc:xacml:1.0:function:and'>
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member-of">
              <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">packard</AttributeValue>
              </Apply>
              <SubjectAttributeDesignator AttributeId="urn:tscp:subject:organization-affiliation"
                    DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Apply>
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member-of">
              <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">program-z</AttributeValue>
              </Apply>
              <SubjectAttributeDesignator AttributeId="urn:tscp:subject:assigned-program"
                    DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Apply>
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member-of">
              <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">DD</AttributeValue>
              </Apply>
              <SubjectAttributeDesignator AttributeId="urn:tscp:subject:assigned-work-effort"
                    DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Apply>
          </Apply>
        </Condition>
      </Rule>

      <Rule RuleId="default-deny-all" Effect="Deny">
        <Description>DENY for all other cases</Description>
      </Rule>
    </Policy>
```

3.5 Demonstrated Business Process

The business scenario that tested by running the 6 steps depicted below:

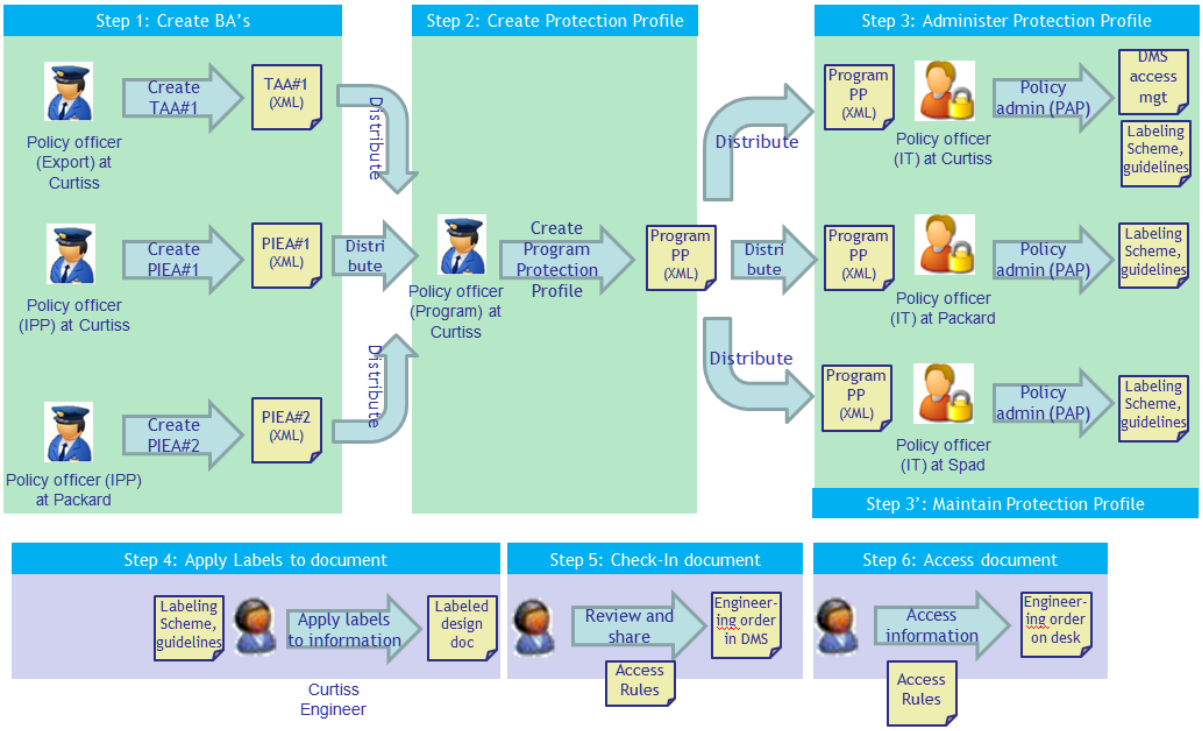

Figure 7: Business scenario test cases

The steps 1 to 3 are administrative steps, whereas steps 4 to 6 are execution steps.

Step 1: Creation of the Business Authorizations

Taken the human-readable representation (Word and PDF documents) of three protection policies (PIEA1, PIEA2, and TAA1) as an input, this step consists in creating the associated Business Authorizations by using the Business Authorization editor tool. The output of this process is made of three XML documents, representing the Business Authorizations in a consistent machine-readable form.

In a real-world implementation, these XML documents should be digitally signed to ensure authenticity and integrity.

Step 2: Creation of the protection profile

The protection profile is created by putting together the business authorizations that need to take place in context of the business scenario, by using the Protection Profile editor tool. The policy officer performing this task typically needs to verify the consistency of the overall result. This consistency may be lacking for various reasons such as utilizations of different namespace to express organization identifiers. The policy officer also adds all the appropriate administrative information that identifies the business context associated to the protection profile. The output of this process is made of a single XML document, representing the protection profile in a machine-readable form, which can be distributed for implementation to all the collaboration partners.

In a real world implementation, there may be a need to filter-out some information depending on the recipient of the protection profile, in order to conceal details such as industrial partnership. Also it is expected that the XML document be digitally signed to ensure authenticity and integrity.

Step 3: Administration of the protection profile

Each organization is then accountable for implementing the protection profile. This implementation covers multiple facets:

- Organizations that need to access shared information need to configure their federation service in order to generate the appropriate attributes about the users, so that these attributes can be retrieved at runtime to perform the authorization decision. The details of the expected attributes are found in the protection profile;

- Organizations that need to host information need to configure the associated enforcement mechanism. In the case of the prototype, Curtiss needs to generate XACML rules from the protection profile, by using the XACML rule generator tool. These organizations also need to configure their federation service in order to retrieve the appropriate attributes from the requestor's federation services at runtime;

- Organizations that produce information need to configure their labelling tool in order to provide them with the knowledge of the available Business Authorization Labels for a given business context. In the case of the prototype, the labelling tool knows how to fetch the available Business Authorizations at runtime by querying the Business Authorization Management System. However there is a need to configure the user-readable aspect of the labels, and this operation needs to be done manually, such as by customizing document templates and associated macros;

- Organizations that produce and consume information need to produce labelling guideline documents and provide the appropriate training and awareness to their employees, in order for them to a) know how to label information and, b) how to handled labelled information in accordance to the attached policies. This part of the procedural enforcement is not shown in the prototype.

Step 4: Application of Business Authorization Labels to a document

A document owner identifies all the Business Authorizations that need to apply to a document, given its context, purpose and contents, and apply the associated Business Authorization Labels accordingly. This process is performed using the labelling tool, which assist the user by providing a search function within the Business Authorization Management System. The output of this process is to generate a document (a Microsoft Word document, in the case of the prototype) that has visual marking and associated machine-readable metadata specifying the Business Authorization Labels.

Step 5: Review and release of a document

An authorized person is in charge of reviewing and validating the business authorization labels set on a document, before authorizing the release of this document. In the real world, the review process should result in the creation of review attributes on the business authorization metadata, most desirably secured using an appropriate cryptographic mechanism, such as a digital signature. The prototype does not demonstrate this step of the process. Once the document's business authorization label is reviewed and cleared for release, the authorized person signs into the Document Management System (Microsoft SharePoint in the prototype), and uploads the document for sharing with other partners. The simple fact to sign in the DMS, navigate to the right document folder, and upload the document, triggers at least three authorization decisions: is the user authorized to access the DMS altogether, is she authorized to access such or such folder, and

is she authorized to upload a document bearing such business authorization label? All three authorizations are performed in accordance to appropriate policies and demonstrated by the prototype.

Step 6: Access to a shared document

A person needs to access a shared document stored in the Document Management System. The person signs into the Document Management System (Microsoft SharePoint in the prototype), locates and downloads the document to her desktop. The simple fact to sign in the DMS, navigate to the right document folder, and download the document, triggers at least three authorization decisions: is the user authorized to access the DMS altogether, is she authorized to access such or such folder, and is she authorized to download a document bearing such business authorization label? All three authorizations are performed in accordance to appropriate policies and demonstrated by the prototype.

Note that once the document is available on the user's desktop, this document is left without any systemic protection. It is up to the user, armed with her training and awareness, to handle the document in accordance with the associated protection policies, based on the human-readable business authorization labels conveyed by the document. A systemic policy enforcement of the document outside of the context of the DMS would require a technology such as Enterprise Digital Right Management, which is outside the scope of the prototype.

4. FURTHER WORK

4.1 Evolution of the Framework

TSCP has formed a group of policy Subject Matter Experts (SME) dedicated to the validation and evolution of the Business Authorization Framework. As a result, the framework is expected to solidify and acquire the robustness required to support more instances of export control and intellectual property protection policies from various policy authorities.

TSCP will engage with the vendor's community in order to obtain the proper Component-off-the-Shelf (COTS) support of the framework, lowering the cost whilst gaining maintainability of the toolset. This will allow organizations to start pilot programs using interoperable products of their choice.

TSCP will also approach various national policy authorities, with the objective to get their buy-in on the utilization of the framework, which ultimately would allow a seamless exchange of policy expressions from the regulator down to the implementers.

4.2 Consistent Protection Across Applications

The implementations of system-based trust infrastructures, which TSCP is looking at in a near future, will be based upon server-side applications. These applications will protect access to documents according to the policy labels, which these documents convey. Accesses to the documents are primarily web-based, such as within Document Management System (DMS). Subsequently TSCP will be looking at other access methods, such as asynchronous access within email applications, or real-time access within web-conferencing applications. The objective is to provide consistent policy enforcement across these various applications, based upon the same information labelling.

4.3 Location Independent Information Protection

One attribute commonly shared by all the server-side applications mentioned above is that systemic information protection is ensured as long as documents reside within the applications. Once a document ends-up on the end-user's desktop environment, it is up to the user to provide procedural protection, based upon the visual aspect of the security label which the document conveys.

TSCP is evaluating several complementary mechanisms to bring systematic enforcement of policies on the user's desktop. These mechanisms include Enterprise Digital Rights Management (EDRM) mechanisms, which allow information assets to be protected regardless of their location. Solutions are available and deployed across organizations, but provide proprietary labelling system, and do not currently offer protection characteristics that are comparable to the ones provided by ABAC policy-engines. TSCP is working with leading technology vendors to fill the gap, in order to provide consistency between location dependent and location independent protection.

4.4 Security Analysis of System-Based Trust Infrastructures

Even if systems capable of fully enforcing the type of organizational policy that need to be enforced (e.g. Intellectual Property or Export Control policies) were available, which again is not the case as of this writing, additional challenges will need to be addressed in order to ensure a full system-based trust. To name a few:

- Issue of correctness: how to prove that a given system enforces a given policy in a correct manner?
- Issue of interoperability: how to ensure that executable policy expressions can be exchanged between different enforcement systems in an interoperable way?
- Issue of policy-expression equivalence: how to prove that two different interpretations (or implementations) of a same policy (possibly using a different policy language) are equivalent?
- Issue of policy selection: in situations of multiple policy candidates, how to ensure that the correct set of policies have been selected for evaluation?
- Issue of policy composition: in situations where multiple policies need to be combined, how to ensure the correctness of the combination?

These challenges will be best addressed by allowing the source of the policy expression and all the generated target implementation forms to be amenable to formal security analysis, in order to allow for model checking and deductive verification. TSCP will naturally seek at leveraging the result of academic research and toolset available, such as NIST Access Control Policy Tool (ACPT) [6] or Margrave [7].

5. REFERENCES

[1] Harrison M., Ruzzo W., Ullman J., "Protection in Operating Systems", Communication of the ACM, pp. 461-471, 1976.

[2] Ferraiolo D.F, Sandhu R., Gavrila S., Kuhn D.R., Chandramouli R., "Proposed NIST Standard for Role-Based Access Control", ACM TISSEC, 4(3):222--274, 2001

[3] Wang L., Wijesekera D., Jajodia S., "A Logic-based Framework for Attribute based Access Control", 2nd ACM Workshop on FMSE, 2004.

[4] Abou El Kalam A., El Baida R., Balbiani P., Benferhat S., "Organisation Based Access Conrol", in Policies for Distributed Systems and Networks, Como, 01/01/03-31/12/03, H. Lutfiyya, J. Moffett, F. Garcia (Eds.), Institute of Electrical and Electronics Engineers, p. 120-131, Jan 2003.

[5] ITAR US Munitions List - http://www.ecustoms.com/vc/usml.cfmXACML – Extensible Access Control Markup Language - http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

[6] NIST – National Institute of Standards and Technology - Access Control Policy Tool (ACPT): http://www.nist.gov/itl/csd/set/acpt.cfm

[7] Brown University et al, Margrave – an API for XACML Policy Verification and Change Analysis: http://www.cs.brown.edu/research/plt/software/margrave/

[8] ITAR US Munitions List - http://www.ecustoms.com/vc/usml.cfm

[9] FIPS 199 – Potential impacts: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf